# Requirements for the protection of software emailed to NIST

## Scope

A number of NIST's evaluation programs require the sending of libraries, executables, and data to NIST. This document establishes exact specifications for the cryptographic protection of such materials. Particularly, it gives procedures for the provider of the software to sign the material to protect integrity and to support NIST in the authenticating the sender. In addition this document gives the mechanism by which the material can be encrypted for confidentiality.

## Submission of software to NIST

NIST requires that all software submitted by the participants be signed and encrypted. Two key pairs are needed:

- Signing is done with the software provider's private key, and
- Encryption is done with NIST's public key, which is published on the NIST evaluation website.

NIST will validate all submitted materials using the participant's public key, and the authenticity of that key will be verified using the key's fingerprint. This fingerprint must be submitted to NIST in writing, normally by writing it on the signed participation agreement.

All cryptographic operations (signing and encrypting) shall be performed with software that implements the OpenPGP standard, as described in the internet RFC 4880. The freely available Gnu Privacy Guard (GPG) software, available at www.gnupg.org, is one such implementation.

The steps below show how to create a public/private key pair and fingerprint using the GPG software.

| **Participant generates their own key** | | |
|---|---|---|
| 1 | Generate your key pair | `$ gpg --gen-key`<br><press Enter for the default type><br><Choose a key size of 2048><br><Choose a non-expiring key><br><Press 'y' then Enter><br><Enter Real Name><br><Enter email address, this is they key identity><br><Enter an optional comment><br><Press 'O' then Enter to continue><br><Enter a passphrase for the secret (private) key><br><br>Once the pair is generated, the key must be exported in the proper format to be sent to NIST. It is crucial that the applicant protect the private key by choosing a strong password that is not shared. |
| 2 | Export your public key | `$ gpg --armor --output forirex.gpg --export <email>`<br><br>where <email> is the address used in Step 1 above; this address is the key identity. The public key will be saved into the file named 'forirex.gpg'. |
| 3 | Email your public key | The file containing the public key must be send to the IREX Test Liaison (irex@nist.gov). |

| | | |
|---|---|---|
| 4 | Write your public key fingerprint on the participation agreement | `$ gpg --fingerprint <email>`<br>The key fingerprint will be shown in the output as a set of hexadecimal digits. The fingerprint must be copied onto the paper participation agreement sent to NIST. |
| **Participant imports NIST's public key**<br>The next series of steps show how the participant will import the IREX public key, and authenticate that key using the key fingerprint. The IREX public key will be sent to each participant after receiving the signed agreement. | | |
| 1 | Import NIST's IREX public key (contained in a file called irex.gpg, for example) | `$ gpg --import irex.gpg <email>`<br>The output should be similar to:<br>`key 856B9B28: public key "IREX Test Liaison (IREX Test Liaison Key) <irex@nist.gov>" imported` |
| 2 | Authenticate the IREX key | `$ gpg --fingerprint irex@nist.gov`<br>The key fingerprint will be shown in the output as a set of hexadecimal digits, which should be<br>A75C EECD EF65 3197 7E66 A960 67D0 4015 407A D929<br>If it is not, contact NIST and do not use the IREX key for encrypting. |
| 3 | Optionally, the participant may want to assign a level of trust to the IREX public key | `$ gpg --edit-key irex@nist.gov`<br><Enter 'trust' at the command prompt><br><Choose a trust level; 3 is a good choice><br><Enter 'y' to approve the trust selection, if asked><br><Press 'q' to quit> |
| **Sending software to NIST**<br>By following the above steps, the keys have been generated and exchanged between NIST and the participant. From this point forward, all software submissions MUST be signed and encrypted. In addition, general email communication can be encrypted and signed, if desired. | | |
| 1 | Encrypt and sign the file to be submitted to NIST | `$ gpg --default-key <email> --output <filename>.gpg --encrypt --recipient irex@nist.gov --sign <filename>`<br><email> is the key identity chosen when the key pair was created.<br><filename> is the file to be submitted to NIST.<br><Enter the passphrase chosen for the private key><br><br>The result shall be emailed to irex@nist.gov. |